

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ  
федеральное государственное автономное образовательное учреждение  
высшего образования  
«Северный (Арктический) федеральный университет имени М.В. Ломоносова»

Высшая школа информационных технологий и автоматизированных систем

**ЛАБОРАТОРНАЯ РАБОТА №4**

По дисциплине: Защита информации в системах управления базами данных

На тему ELK

Выполнил обучающийся:  
Грозов Илья Владимирович

Направление подготовки / специальность:  
10.03.01 Информационная безопасность

Курс: 3  
Группа: 151113

Руководитель: Зубарев Александр Андреевич, ст.  
преподаватель

Отметка о зачете \_\_\_\_\_

Руководитель \_\_\_\_\_ А.А. Зубарев.

Архангельск 2024

## ЗАДАНИЕ

Получить практический навык при работе с ELK

## ХОД РАБОТЫ

### 1. ELK

#### 1.1 Конфигурация контейнера с docker

На момент выполнения данной работы установка и работа с docker невозможна. Работа будет выполнена на виртуальной машине с именем huguenot-lr4. Перед установкой выполним установку java при помощи команды: `sudo apt install-jre`. Установка java отображена на рисунке 1

```
root@ZIVSYBD-LR4:/home/huguenot-lr4# sudo apt install default-jre
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  ca-certificates-java default-jre-headless java-common libatk-wrapper-java
  libatk-wrapper-java-jni openjdk-11-jre openjdk-11-jre-headless
Suggested packages:
  fonts-ipafont-gothic fonts-ipafont-mincho fonts-wqy-microhei
  | fonts-wqy-zenhei fonts-indic
The following NEW packages will be installed:
  ca-certificates-java default-jre default-jre-headless java-common
  libatk-wrapper-java libatk-wrapper-java-jni openjdk-11-jre
  openjdk-11-jre-headless
0 upgraded, 8 newly installed, 0 to remove and 0 not upgraded.
Need to get 38.6 MB of archives.
After this operation, 177 MB of additional disk space will be used.
Do you want to continue? [Y/n]
```

Рисунок 1 – Установка java

Завершение установки java на виртуальную машину отображено на рисунке 2

```
Processing triggers for mailcap (3.69) ...
Processing triggers for desktop-file-utils (0.26-1) ...
Processing triggers for hicolor-icon-theme (0.17-2) ...
Processing triggers for gnome-menus (3.36.0-1) ...
Processing triggers for man-db (2.9.4-2) ...
Processing triggers for ca-certificates (20210119) ...
Updating certificates in /etc/ssl/certs...
0 added, 0 removed; done.
Running hooks in /etc/ca-certificates/update.d...

done.
done.
root@ZiVSYBD-LR4:/home/huguenot-lr4#
```

Рисунок 2 – Завершение установки java

Для работы с пакетами deb необходимо выполнить установку apt-transport-https. Выполним установку apt-transport-https при помощи команды: `sudo apt install apt-transport-https`. Установка apt-transport-https отображена на рисунке 3

```
root@ZiVSYBD-LR4:/home/huguenot-lr4# apt install apt-transport-https
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  apt-transport-https
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 160 kB of archives.
After this operation, 166 kB of additional disk space will be used.
Get:1 http://deb.debian.org/debian bullseye/main amd64 apt-transport-https all 2.2.4 [160 kB]
Fetched 160 kB in 0s (432 kB/s)
Selecting previously unselected package apt-transport-https.
(Reading database ... 165828 files and directories currently installed.)
Preparing to unpack .../apt-transport-https_2.2.4_all.deb ...
Unpacking apt-transport-https (2.2.4) ...
Setting up apt-transport-https (2.2.4) ...
root@ZiVSYBD-LR4:/home/huguenot-lr4#
```

Рисунок 3 – Установка apt-transport-https

ElasticSearch невозможно загрузить и установить из России. Воспользуемся зеркалом. Добавим репозиторий в систему при помощи команды: `echo "deb http://elasticrepo.serveradmin.ru bullseye main" | tee /etc/apt/sources.list.d/elasticrepo.list`. Добавление репозитория в систему отображено на рисунке 4

```
root@ZIVSYBD-LR4:/home/huguenot-lr4# echo "deb http://elasticrepo.serveradmin.ru bullseye main" | tee /etc/apt/sources.list.d/elasticrepo.list
deb http://elasticrepo.serveradmin.ru bullseye main
root@ZIVSYBD-LR4:/home/huguenot-lr4#
```

## Рисунок 4 – Добавление репозитория в систему

Добавим apt ключ при помощи команды: `wget -qO - http://elasticrepo.serveradmin.ru/elastic.asc | apt-key add -`. Добавление ключа отображено на рисунке 5

```
root@ZIVSYBD-LR4:/home/huguenot-lr4# wget -qO - http://elasticrepo.serveradmin.ru/elastic.asc | apt-key add -
Warning: apt-key is deprecated. Manage keyring files in trusted.gpg.d instead (see apt-key(8)).
OK
root@ZIVSYBD-LR4:/home/huguenot-lr4#
```

## Рисунок 5 – Добавление ключа

Выполним установку из добавленного репозитория при помощи команды: `apt update && apt install elasticsearch`. Выполнение установки из репозитория отображено на рисунке 6

```
root@ZIVSYBD-LR4:/home/huguenot-lr4# apt update && apt install elasticsearch
Hit:1 http://security.debian.org/debian-security bullseye-security InRelease
Hit:2 http://deb.debian.org/debian bullseye InRelease
Hit:3 http://deb.debian.org/debian bullseye-updates InRelease
Get:4 http://elasticrepo.serveradmin.ru bullseye InRelease [4,313 B]
Get:5 http://elasticrepo.serveradmin.ru bullseye/main amd64 Packages [2,399 B]
Fetched 6,712 B in 1s (5,540 B/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
All packages are up to date.
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  elasticsearch
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 576 MB of archives.
After this operation, 1,136 MB of additional disk space will be used.
Get:1 http://elasticrepo.serveradmin.ru bullseye/main amd64 elasticsearch amd64 8.13.3 [576 MB]
2% [1 elasticsearch 12.6 MB/576 MB 2%]
```

## Рисунок 6 – Выполнение установки из репозитория

Процесс установки отображен на рисунке 7

```
Creating elasticsearch group... OK
Creating elasticsearch user... OK
Unpacking elasticsearch (8.13.3) ...
Setting up elasticsearch (8.13.3) ...
Progress: [ 60%] [#####]
```

## Рисунок 7 – Процесс установки

Добавим ElasticSearch в автозагрузку при помощи последовательного выполнения команд: `systemctl daemon-reload`, `systemctl enable elasticsearch.service`, `systemctl start elasticsearch.service`. Добавление ElasticSearch в автозагрузку отображено на рисунке 8

```
root@ZIVSYBD-LR4:/home/huguenot-lr4# systemctl daemon-reload
root@ZIVSYBD-LR4:/home/huguenot-lr4# systemctl enable elasticsearch.service
Created symlink /etc/systemd/system/multi-user.target.wants/elasticsearch.service → /lib/systemd/system/elasticsearch.service.
root@ZIVSYBD-LR4:/home/huguenot-lr4# systemctl start elasticsearch.service
root@ZIVSYBD-LR4:/home/huguenot-lr4#
```

## Рисунок 8 – Добавление ElasticSearch в автозагрузку

При помощи команды `systemctl status elasticsearch.service` проверим запустился ли ElasticSearch. Проверка запуска ElasticSearch отображена на рисунке 9

```
root@ZIVSYBD-LR4:/home/huguenot-lr4# systemctl status elasticsearch.service
● elasticsearch.service - Elasticsearch
   Loaded: loaded (/lib/systemd/system/elasticsearch.service; enabled; vendor preset: enabled)
   Active: active (running) since Tue 2024-06-04 18:24:03 MSK; 1min 0s ago
     Docs: https://www.elastic.co
   Main PID: 7416 (java)
    Tasks: 82 (limit: 19095)
   Memory: 8.3G
      CPU: 1min 15.005s
   CGroup: /system.slice/elasticsearch.service
           └─7416 /usr/share/elasticsearch/jdk/bin/java -Xms4m -Xmx64m -XX:+UseSerialGC -Dcli.name=server -Dcli.script=/usr/share>
           └─7477 /usr/share/elasticsearch/jdk/bin/java -Des.networkaddress.cache.ttl=60 -Des.networkaddress.cache.negative.ttl=1>
           └─7507 /usr/share/elasticsearch/modules/x-pack-ml/platform/linux-x86_64/bin/controller

Jun 04 18:23:36 ZIVSYBD-LR4 systemd[1]: Starting Elasticsearch...
Jun 04 18:23:46 ZIVSYBD-LR4 systemd-entrypoint[7416]: Jun 04, 2024 6:23:46 PM sun.util.locale.provider.LocaleProviderAdapter <clini>
Jun 04 18:23:46 ZIVSYBD-LR4 systemd-entrypoint[7416]: WARNING: COMPAT locale provider will be removed in a future release
Jun 04 18:24:03 ZIVSYBD-LR4 systemd[1]: Started Elasticsearch.
lines 1-17/17 (END)
```

## Рисунок 9 – Проверка запуска ElasticSearch

ElasticSearch запущен. Для дальнейшей работы нам потребуется выполним установку `curl` при помощи команды: `apt-get install curl`. Установка `curl` отображена на рисунке 10

```

root@ZIVSYBD-LR4:/home/huguenot-lr4# apt-get install curl
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  curl
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 271 kB of archives.
After this operation, 440 kB of additional disk space will be used.
Get:1 http://deb.debian.org/debian bullseye/main amd64 curl amd64 7.74.0-1.3+deb11u11 [271 kB]
Fetched 271 kB in 0s (732 kB/s)
Selecting previously unselected package curl.
(Reading database ... 167174 files and directories currently installed.)
Preparing to unpack .../curl_7.74.0-1.3+deb11u11_amd64.deb ...
Unpacking curl (7.74.0-1.3+deb11u11) ...
Setting up curl (7.74.0-1.3+deb11u11) ...
Processing triggers for man-db (2.9.4-2) ...
root@ZIVSYBD-LR4:/home/huguenot-lr4#

```

Рисунок 10 – Установка curl

После установки curl выполним запрос к Elasticsearch при помощи команды: `curl -k --user elastic:'N0f4jpvLM2WxQILMMMWM'` `https://127.0.0.1:9200`. Ответ кластера отображен на рисунке 11

```

root@ZIVSYBD-LR4:/home/huguenot-lr4# curl -k --user elastic:'N0f4jpvLM2WxQILMMMWM' https://127.0.0.1:9200
{
  "name" : "ZIVSYBD-LR4",
  "cluster_name" : "elasticsearch",
  "cluster_uuid" : "BMAJ0L0iS_ae8os0KkIqcw",
  "version" : {
    "number" : "8.13.3",
    "build_flavor" : "default",
    "build_type" : "deb",
    "build_hash" : "617f7b76c4ebcb5a7f1e70d409a99c437c896aea",
    "build_date" : "2024-04-29T22:05:16.051731935Z",
    "build_snapshot" : false,
    "lucene_version" : "9.10.0",
    "minimum_wire_compatibility_version" : "7.17.0",
    "minimum_index_compatibility_version" : "7.0.0"
  },
  "tagline" : "You Know, for Search"
}
root@ZIVSYBD-LR4:/home/huguenot-lr4#

```

Рисунок 11 – Ответ кластера

## 1.2 Установка паролей и логинов к системе

Для создания пользователей, установки логинов и паролей в системе нам необходимо дополнительно установить curl jq при помощи команды `apt-get install curl jq`. Выполнение установки curl jq отображено на рисунке 12

```

root@ZiVSYBD-LR4:/home/huguenot-lr4# apt-get install curl jq
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
curl is already the newest version (7.74.0-1.3+deb11u11).
The following additional packages will be installed:
  libjq1 libonig5
The following NEW packages will be installed:
  jq libjq1 libonig5
0 upgraded, 3 newly installed, 0 to remove and 0 not upgraded.
Need to get 384 kB of archives.
After this operation, 1,148 kB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://deb.debian.org/debian bullseye/main amd64 libonig5 amd64 6.9.6-1.1 [185 kB]
Get:2 http://deb.debian.org/debian bullseye/main amd64 libjq1 amd64 1.6-2.1 [135 kB]
Get:3 http://deb.debian.org/debian bullseye/main amd64 jq amd64 1.6-2.1 [64.9 kB]
Fetched 384 kB in 0s (904 kB/s)
Selecting previously unselected package libonig5:amd64.
(Reading database ... 167182 files and directories currently installed.)
Preparing to unpack .../libonig5_6.9.6-1.1_amd64.deb ...
Unpacking libonig5:amd64 (6.9.6-1.1) ...
Selecting previously unselected package libjq1:amd64.
Preparing to unpack .../libjq1_1.6-2.1_amd64.deb ...
Unpacking libjq1:amd64 (1.6-2.1) ...
Selecting previously unselected package jq.
Preparing to unpack .../archives/jq_1.6-2.1_amd64.deb ...
Unpacking jq (1.6-2.1) ...
Setting up libonig5:amd64 (6.9.6-1.1) ...
Setting up libjq1:amd64 (1.6-2.1) ...
Setting up jq (1.6-2.1) ...
Processing triggers for man-db (2.9.4-2) ...

```

Рисунок 12 – Выполнение установки curl jq

Во время создания пользователей был ошибочно создан пользователь по команде листинга 1

### Листинг 1 – Команда

```

curl -k --user elastic:elastic123 -X POST
"https://192.168.100.7:9200/_security/user/bruno?pretty" -H 'Content-Type:
application/json' -d'
{
  "password" : "kamisama123",
  "roles" : [ "superuser" ],
  "full_name" : "Bruno Ricci",
  "email" : "bruno@techexpert.tips"
}
'
```

Ошибочное создание пользователя отображено на рисунке 13

```

root@ZiVSYBD-LR4:/home/huguenot-lr4# curl -k --user elastic:'N0f4jpvLM2wxQILM000M' https://127.0.0.1:9200/_security/user/bruno?pretty
root@ZiVSYBD-LR4:/home/huguenot-lr4# curl -k --user elastic:'N0f4jpvLM2wxQILM000M' https://127.0.0.1:9200/_security/user/bruno?pretty -H 'Content-Type: application/json' -d'
{"password": "kamisama123", "roles": [ "superuser" ], "full_name": "Bruno Ricci", "email": "bruno@techexpert.tips"}
root@ZiVSYBD-LR4:/home/huguenot-lr4# curl -k --user elastic:'N0f4jpvLM2wxQILM000M' https://127.0.0.1:9200/_security/user/bruno?pretty
{"created": true}

```



### Рисунок 13 – Ошибочное создание пользователя

Создание нового пользователя было невозможно. Виртуальная машина была возвращена в состояние до изменения настроек пользователя. В дальнейшем была использована предыдущая команда для создания пользователя huguenot. Создание пользователя huguenot отображено на рисунке 14

```
root@ZivSYBD-LR4:/home/huguenot-lr4# curl -k --user elastic:N0f4jpvLM2WxQILWMM -X POST "https://127.0.0.1:9200/_security/user/bruno?pretty" -H 'Content-Type: application/json' -d '{
  "password" : "huguenot123",
  "roles" : [ "superuser" ],
  "full_name" : "huguenot huguenot",
  "email" : "huguenot@huguenot.com"
}'
{
  "created" : true
}
root@ZivSYBD-LR4:/home/huguenot-lr4#
```

### Рисунок 14 – Создание пользователя huguenot

При попытке авторизации было выяснено, что huguenot не является именем пользователя им остается bruno. Данные в команде об имени пользователя не изменялись. Пошлем запрос к Elasticsearch при помощи команды `curl -k --user bruno:huguenot123 -X GET "https://127.0.0.1:9200/_security/user?pretty"` с именем пользователя bruno и паролем huguenot123. Выполнение запроса к Elasticsearch от пользователя bruno отображен на рисунке 15

```
root@ZivSYBD-LR4:/home/huguenot-lr4# curl -k --user bruno:huguenot123 -X GET "https://127.0.0.1:9200/_security/user?pretty"
```

### Рисунок 15 – Выполнение запроса к Elasticsearch от пользователя bruno

Мы получили информацию о пользователях в системе. Ответ на запрос отображен на рисунке 16

```

"remote_monitoring_user" : {
  "username" : "remote_monitoring_user",
  "roles" : [
    "remote_monitoring_collector",
    "remote_monitoring_agent"
  ],
  "full_name" : null,
  "email" : null,
  "metadata" : {
    "_reserved" : true
  },
  "enabled" : true
},
"bruno" : {
  "username" : "bruno",
  "roles" : [
    "superuser"
  ],
  "full_name" : "huguenot huguenot",
  "email" : "huguenot@huguenot.com",
  "metadata" : { },
  "enabled" : true
}
}
root@ZIVSYBD-LR4:/home/huguenot-lr4#

```

Рисунок 16 – Ответ на запрос

### 1.3 Изменение параметров cluster\_name

Чтобы изменить имя кластера воспользуемся командой: `nano /etc/elasticsearch/elasticsearch.yml`. Необходимо выполнить редактирование конфигурационного файла. Открытие файла отображено на рисунке 17

```

root@ZIVSYBD-LR4:/home/huguenot-lr4# nano /etc/elasticsearch/elasticsearch.yml

```

Рисунок 17 – Открытие конфигурационного файла

В файле `elasticsearch.yml` изменим строку `cluster.name` предварительно раскомментировав ее. Изменим название на `huhguenotcluster`. Изменение названия кластера отображено на рисунке 18

```
huguenot-lr4@ZlvSYBD-LR4: ~
GNU nano 5.4 /etc/elasticsearch/elasticsearch.yml *
# ===== Elasticsearch Configuration =====
#
# NOTE: Elasticsearch comes with reasonable defaults for most settings.
#       Before you set out to tweak and tune the configuration, make sure you
#       understand what are you trying to accomplish and the consequences.
#
# The primary way of configuring a node is via this file. This template lists
# the most important settings you may want to configure for a production cluster.
#
# Please consult the documentation for further information on configuration options:
# https://www.elastic.co/guide/en/elasticsearch/reference/index.html
#
# ----- Cluster -----
#
# Use a descriptive name for your cluster:
#
cluster.name: huguenotcluster
#
# ----- Node -----
#
```

Рисунок 18 – Изменение название кластера

Для вступления в силу изменений остановим Elasticsearch при помощи команды `systemctl stop elasticsearch.service` и запустим его при помощи команды `systemctl start elasticsearch.service`. Остановка и запуск Elasticsearch отображены на рисунке 19

```
root@ZlvSYBD-LR4:/home/huguenot-lr4# systemctl stop elasticsearch.service
root@ZlvSYBD-LR4:/home/huguenot-lr4# systemctl start elasticsearch.service
```

Рисунок 19 – Остановка и запуск Elasticsearch

При помощи команды `systemctl status elasticsearch.service` проверим запустился ли Elasticsearch. Проверка запуска Elasticsearch отображена на рисунке 20

```
root@ZlvSYBD-LR4:/home/huguenot-lr4# systemctl status elasticsearch.service
● elasticsearch.service - Elasticsearch
   Loaded: loaded (/lib/systemd/system/elasticsearch.service; enabled; vendor preset: enabled)
   Active: active (running) since Tue 2024-06-04 18:36:15 MSK; 6s ago
     Docs: https://www.elastic.co
  Main PID: 8366 (java)
    Tasks: 86 (limit: 19095)
   Memory: 8.3G
      CPU: 42.224s
   CGroup: /system.slice/elasticsearch.service
           └─8366 /usr/share/elasticsearch/jdk/bin/java -Xms4m -Xmx64m -XX:+UseSerialGC -Dcli.name=server -Dcli.scrip>
             └─8428 /usr/share/elasticsearch/jdk/bin/java -Des.networkaddress.cache.ttl=60 -Des.networkaddress.cache.n>
               └─8451 /usr/share/elasticsearch/modules/x-pack-ml/platform/linux-x86_64/bin/controller

Jun 04 18:35:59 ZlvSYBD-LR4 systemd[1]: Starting Elasticsearch...
Jun 04 18:36:02 ZlvSYBD-LR4 systemd-entrypoint[8366]: Jun 04, 2024 6:36:02 PM sun.util.locale.provider.LocaleProviderA>
Jun 04 18:36:02 ZlvSYBD-LR4 systemd-entrypoint[8366]: WARNING: COMPAT locale provider will be removed in a future rele>
Jun 04 18:36:15 ZlvSYBD-LR4 systemd[1]: Started Elasticsearch.
lines 1-17/17 (END)
```

Рисунок 20 – Проверка запуска Elasticsearch

Выполним запрос к кластеру для проверки смены его имени при помощи команды: `curl -k --user elastic:N0f4jpvLM2WxQILMMMWM -X GET https://127.0.0.1:9200` Проверка смены имени кластера отображена на рисунке 21

```
root@ZiVSYBD-LR4:/home/huguenot-lr4# curl -k --user elastic:'N0f4jpvLM2WxQILMMMWM' https://127.0.0.1:9200
{
  "name" : "ZiVSYBD-LR4",
  "cluster_name" : "huguenotcluster",
  "cluster_uuid" : "BMAJ0L0iS_ae8os0KkIqcw",
  "version" : {
    "number" : "8.13.3",
    "build_flavor" : "default",
    "build_type" : "deb",
    "build_hash" : "617f7b76c4ebcb5a7f1e70d409a99c437c896aea",
    "build_date" : "2024-04-29T22:05:16.051731935Z",
    "build_snapshot" : false,
    "lucene_version" : "9.10.0",
    "minimum_wire_compatibility_version" : "7.17.0",
    "minimum_index_compatibility_version" : "7.0.0"
  },
  "tagline" : "You Know, for Search"
}
```

Рисунок 21 – Проверка смены имени кластера

Для альтернативного способа проверки имени кластера можно воспользоваться командой: `curl -k --user elastic:N0f4jpvLM2WxQILMMMWM -X GET "https://127.0.0.1:9200/_security/_cluster/health?pretty"` Альтернативный способ проверки имени кластера отображен на рисунке 22

```
root@ZiVSYBD-LR4:/home/huguenot-lr4# curl -k --user elastic:'N0f4jpvLM2WxQILMMMWM' https://127.0.0.1:9200/_cluster/health?pretty
{
  "cluster_name" : "huguenotcluster",
  "status" : "green",
  "timed_out" : false,
  "number_of_nodes" : 1,
  "number_of_data_nodes" : 1,
  "active_primary_shards" : 1,
  "active_shards" : 1,
  "relocating_shards" : 0,
  "initializing_shards" : 0,
  "unassigned_shards" : 0,
  "delayed_unassigned_shards" : 0,
  "number_of_pending_tasks" : 0,
  "number_of_in_flight_fetch" : 0,
  "task_max_waiting_in_queue_millis" : 0,
  "active_shards_percent_as_number" : 100.0
}
```

Рисунок 22 – Альтернативный способ проверки имени кластера

## 1.4 Дополнительные настройки и конфигурация Elasticsearch

Данный раздел зарезервирован под дополнительную настройку Elasticsearch для связи с другими приложениями

## 2 KIBANA

### 2.1 Установка kibana

Добавим публичный ключ Kibana в систему при помощи команды: `wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | apt-key add` – Добавление публичного ключа Kibana отображено на рисунке 23

```
root@ZIVSYBD-LR4:/home/huguenot-lr4# wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | apt-key add -  
Warning: apt-key is deprecated. Manage keyring files in trusted.gpg.d instead (see apt-key(8)).  
gpg: no valid OpenPGP data found.
```

Рисунок 23 – Добавление публичного ключа Kibana

Если официальный репозиторий недоступен, добавим репозиторий с зеркала при помощи команды: `echo "deb http://elasticrepo.serveradmin.ru bullseye main" | tee /etc/apt/sources.list.d/elasticrepo.list` Добавление репозитория Kibana с зеркала в систему отображено на рисунке 24

```
root@ZIVSYBD-LR4:/home/huguenot-lr4# echo "deb http://elasticrepo.serveradmin.ru bullseye main" | tee /etc/apt/sources.list.d/elasticrepo.list  
deb http://elasticrepo.serveradmin.ru bullseye main
```

Рисунок 24 – Добавление репозитория Kibana с зеркала в систему

Для добавления публичного ключа Kibana с зеркала воспользуемся командой: `wget -qO - http://elasticrepo.serveradmin.ru/elastic.asc | apt-key add` – Добавление публичного ключа Kibana с зеркала отображено на рисунке 25

```
root@ZIVSYBD-LR4:/home/huguenot-lr4# wget -qO - http://elasticrepo.serveradmin.ru/elastic.asc | apt-key add -  
Warning: apt-key is deprecated. Manage keyring files in trusted.gpg.d instead (see apt-key(8)).  
OK
```

Рисунок 25 – Добавление публичного ключа Kibana с зеркала

Выполним установку Kibana при помощи команды: `apt install kibana`. Выполнение установки Kibana отображена на рисунке 26

```

root@ZivSYBD-LR4:/home/huguenot-lr4# apt update && apt install kibana
Hit:1 http://security.debian.org/debian-security bullseye-security InRelease
Hit:2 http://deb.debian.org/debian bullseye InRelease
Hit:3 http://deb.debian.org/debian bullseye-updates InRelease
Hit:4 http://elasticrepo.serveradmin.ru bullseye InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
All packages are up to date.
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  kibana
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 321 MB of archives.
After this operation, 938 MB of additional disk space will be used.
Get:1 http://elasticrepo.serveradmin.ru bullseye/main amd64 kibana amd64 8.13.3 [321 MB]
Fetched 321 MB in 35s (9,087 kB/s)
Selecting previously unselected package kibana.
(Reading database ... 167202 files and directories currently installed.)
Preparing to unpack .../kibana_8.13.3_amd64.deb ...
Unpacking kibana (8.13.3) ...
Setting up kibana (8.13.3) ...
Creating kibana group... OK
Creating kibana user... OK
Kibana is currently running with legacy OpenSSL providers enabled! For details and instructions on how to disable see https://www.elastic.co/guide/en/kibana/8.13/production.html#openssl-legacy-provider
Created Kibana keystore in /etc/kibana/kibana.keystore
root@ZivSYBD-LR4:/home/huguenot-lr4#

```

Рисунок 26 – Выполнение установки Kibana

Дополнительно произведем установку утилиты net-tools. Установка утилиты net-tools отображена на рисунке 27

```

root@ZivSYBD-LR4:/home/huguenot-lr4# apt install net-tools
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  net-tools
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 250 kB of archives.
After this operation, 1,015 kB of additional disk space will be used.
Get:1 http://deb.debian.org/debian bullseye/main amd64 net-tools amd64 1.60+git20181103.0eebece-1 [250 kB]
Fetched 250 kB in 0s (672 kB/s)
Selecting previously unselected package net-tools.
(Reading database ... 257467 files and directories currently installed.)
Preparing to unpack .../net-tools_1.60+git20181103.0eebece-1_amd64.deb ...
Unpacking net-tools (1.60+git20181103.0eebece-1) ...
Setting up net-tools (1.60+git20181103.0eebece-1) ...
Processing triggers for man-db (2.9.4-2) ...

```

Рисунок 27 – Установка утилиты net-tools

При помощи последовательного выполнения команд: `systemctl daemon-reload`, `systemctl enable kibana.service`, `systemctl start kibana.servic` добавим kibana в автозагрузку и запусти его

При помощи команды: `netstat -tulnp | grep 5601` что Kibana запущена на порту 5601. Проверка запуска Kibana на порту 5601 отображена на рисунке 28

```

root@ZivSYBD-LR4:/home/huguenot-lr4# netstat -tulnp | grep 5601
tcp        0      0 127.0.0.1:5601        0.0.0.0:*               LISTEN      13113/node

```

Рисунок 28 - Проверка запуска Kibana на порту 5601

Выполним GET запрос к Kibana при помощи команды: `curl -X GET http://127.0.0.1:5601/_security /_cluster/health?pretty`. Результат выполненного запроса отображен на рисунке 29

```

root@ZIVSYBD-LR4:/home/huguenot-lr4# curl -X GET http://127.0.0.1:5601/_security/_cluster/health?pretty
<!DOCTYPE html><html lang="en"><head><meta charset="utf-8"><meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1"><meta name="viewport" content="width=device-width"><title>Elastic</title><style>
  @font-face {
    font-family: 'Inter';
    font-style: normal;
    font-weight: 100;
    src: url('/003e4a429463/ui/fonts/inter/Inter-Thin.woff2') format('woff2'), url('/003e4a429463/ui/fonts/inter/Inter-Thin.woff') format('woff');
  }
  @font-face {
    font-family: 'Inter';
    font-style: italic;
    font-weight: 100;
    src: url('/003e4a429463/ui/fonts/inter/Inter-ThinItalic.woff2') format('woff2'), url('/003e4a429463/ui/fonts/inter/Inter-ThinItalic.woff') format('woff');
  }
  @font-face {
    font-family: 'Inter';
    font-style: normal;
    font-weight: 200;
    src: url('/003e4a429463/ui/fonts/inter/Inter-ExtraLight.woff2') format('woff2'), url('/003e4a429463/ui/fonts/inter/Inter-ExtraLight.woff') format('woff');
  }
  @font-face {
    font-family: 'Inter';
    font-style: italic;
    font-weight: 200;
    src: url('/003e4a429463/ui/fonts/inter/Inter-ExtraLightItalic.woff2') format('woff2'), url('/003e4a429463/ui/fonts/inter/Inter-ExtraLightItalic.woff') format('woff');
  }

```

Рисунок 29 – Результат выполненного запроса

## 2.1 Настройка Kibana

Для настройки Kibana выполним редактирование файла конфигурации при помощи команды: `nano /etc/kibana/kibana.yml`. Открытие файла конфигурации отображено на рисунке 30

```

root@ZIVSYBD-LR4:/home/huguenot-lr4# nano /etc/kibana/kibana.yml
root@ZIVSYBD-LR4:/home/huguenot-lr4#

```

Рисунок 30 – Открытие файла конфигурации

Раскомментируем параметр `server.host` и укажем адрес `0.0.0.0` чтобы было прослушивание всех соединений. Редактирование параметра `server.host` отображено на рисунке 31

```

GNU nano 5.4 /etc/kibana/kibana.yml *
# For more configuration options see the configuration guide for Kibana in
# https://www.elastic.co/guide/index.html

# ===== System: Kibana Server =====
# Kibana is served by a back end server. This setting specifies the port to use.
#server.port: 5601

# Specifies the address to which the Kibana server will bind. IP addresses and host names are both valid values.
# The default is 'localhost', which usually means remote machines will not be able to connect.
# To allow connections from remote users, set this parameter to a non-loopback address.
server.host: "0.0.0.0"

```

Рисунок 31 – Редактирование параметра

Выполним перезагрузку. При помощи команды: `/usr/share/elasticsearch/bin/elasticsearch-reset-password -u kibana_system` создадим пароль для встроенного пользователя `kibana_system`. Создание пароля для пользователя `kibana_system` отображено на рисунке 32

```

root@ZIVSYBD-LR4:/home/huguenot-lr4# /usr/share/elasticsearch/bin/elasticsearch-reset-password -u kibana_system
This tool will reset the password of the [kibana_system] user to an autogenerated value.
The password will be printed in the console.
Please confirm that you would like to continue [y/N]y

Password for the [kibana_system] user successfully reset.
New value: bNFThR8kXMr82oKRp2pm
root@ZIVSYBD-LR4:/home/huguenot-lr4#

```

Рисунок 32 – Создание пароля для пользователя kibana\_system

Укажем автоматически сгенерированный сертификат во время установки elasticsearch. Выполним копирование созданного сертификата из директории /etc/elasticsearch/certs в директорию /etc/kibana при помощи команды: `cp -R /etc/elasticsearch/certs /etc/kibana`. Для прав используем команду: `chown -R root:kibana /etc/kibana/certs`. Копирование сертификатов и настройка прав отображено на рисунке 33

```

root@ZIVSYBD-LR4:/home/huguenot-lr4# cp -R /etc/elasticsearch/certs /etc/kibana
root@ZIVSYBD-LR4:/home/huguenot-lr4# chown -R root:kibana /etc/kibana/certs
root@ZIVSYBD-LR4:/home/huguenot-lr4# █

```

Рисунок 33 – Копирование сертификатов и настройка прав

В ранее изменяемом конфигурационном файле kibana добавив информацию о сертификате. Добавление информации о сертификате в конфигурационный файл kibana отображена на рисунке 34

```

# Enables you to specify a path to the PEM file for the certificate
# authority for your Elasticsearch instance.
elasticsearch.ssl.certificateAuthorities: [ "/etc/kibana/certs/http_ca.crt" ]

```

Рисунок 34 – Добавление информации о сертификате в конфигурационный файл kibana

В конфигурационный файл kibana добавим учетную запись пользователя kibana\_system со сгенерированным паролем. Добавление учетной записи пользователя kibana\_system со сгенерированным паролем отображена на рисунке 35



```
# If your Elasticsearch is protected with basic authentication, these settings provide
# the username and password that the Kibana server uses to perform maintenance on the Kibana
# index at startup. Your Kibana users still need to authenticate with Elasticsearch, which
# is proxied through the Kibana server.
elasticsearch.username: "kibana_system"
elasticsearch.password: "bNFTThR8kXMr82oKRp2pm"
```

Рисунок 35 – Добавление учетной записи пользователя kibana\_system со сгенерированным паролем

В конфигурационный файл kibana укажем подключение по HTTPS. Указание подключения по HTTPS в конфигурационном файле kibana отображено на рисунке 36

```
# ===== System: Elasticsearch =====
# The URLs of the Elasticsearch instances to use for all your queries.
elasticsearch.hosts: ["https://localhost:9200"]
```

Рисунок 36 – Указание подключения по HTTPS в конфигурационном файле kibana

После чего перезагрузим kibana при помощи команды: `systemctl restart kibana.service`

Зайдем в web – интерфейс по адресу: 127.0.0.1:5601. Вход в интерфейс по адресу 127.0.0.1:5601 отображен на рисунке 37

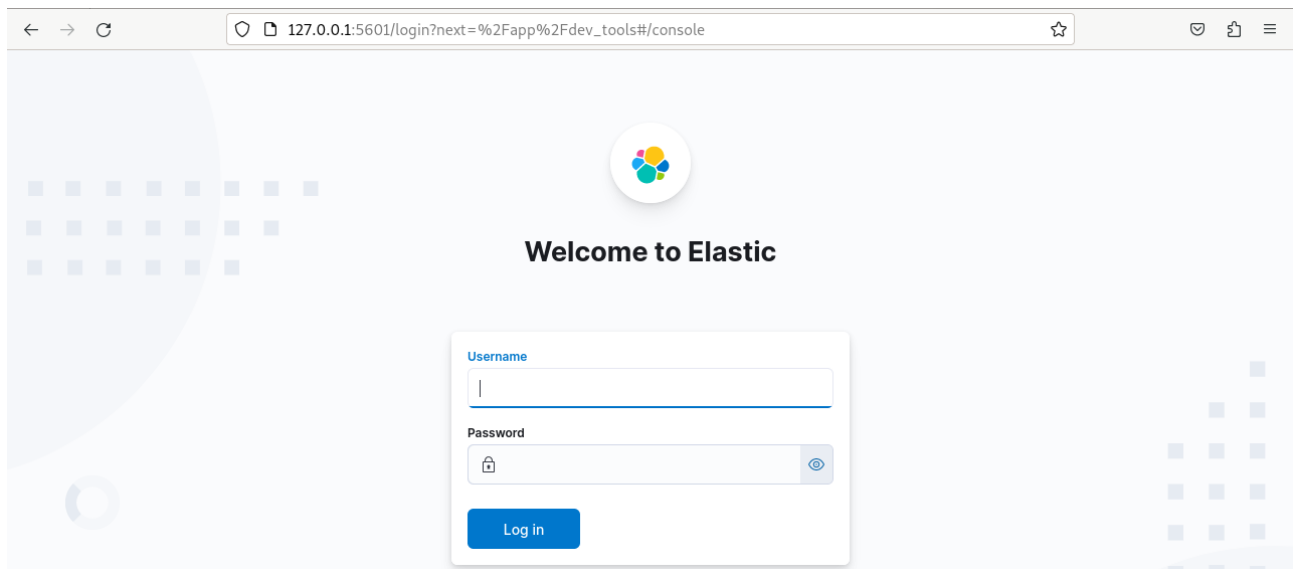


Рисунок 37 – Вход в интерфейс по адресу 127.0.0.1:5601

Вход выполняется под учетной записью elastic.

### 2.3 Составление и отправка запросов

Выполним тестовый запрос предложенный elastic. Предложенный запрос отображен на рисунке 38

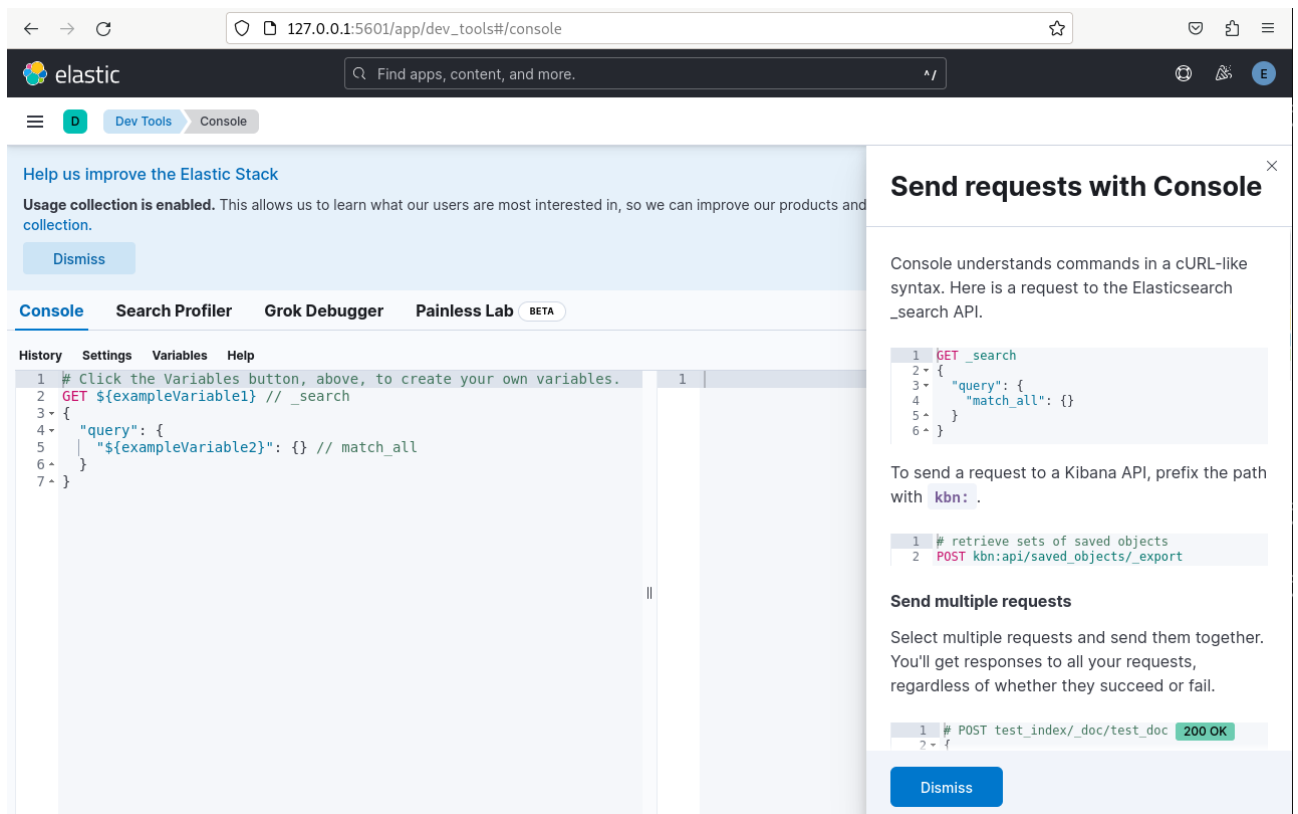


Рисунок 38 – Предложенный запрос

Результат выполненного тестового предложенного запроса отображен на рисунке 39

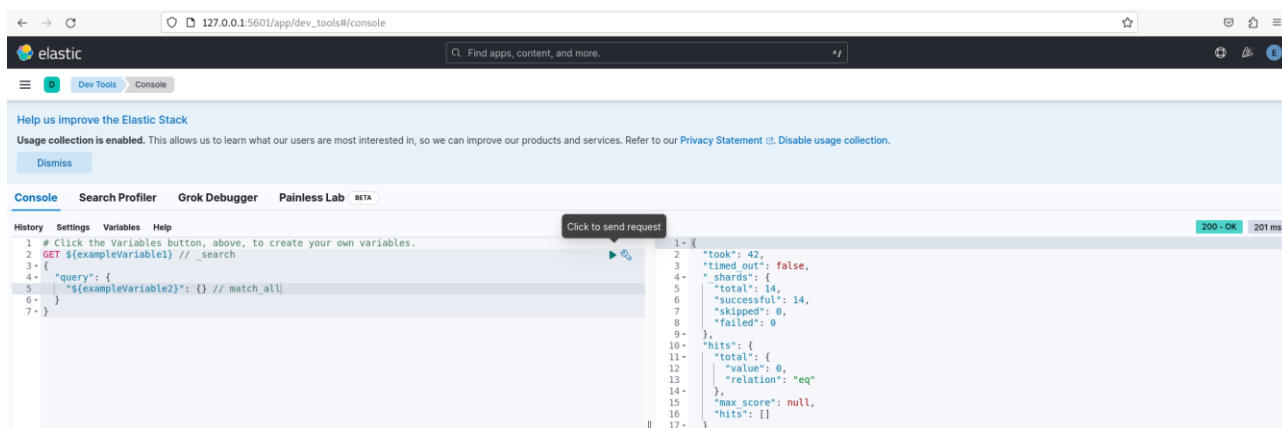


Рисунок 39 – Результат выполненного тестового предложенного запроса

Выполним запрос предложенный лабораторной работой. Предложенный запрос: GET /\_cluster/health?pretty. Результат выполненного запроса отображен на рисунке 40

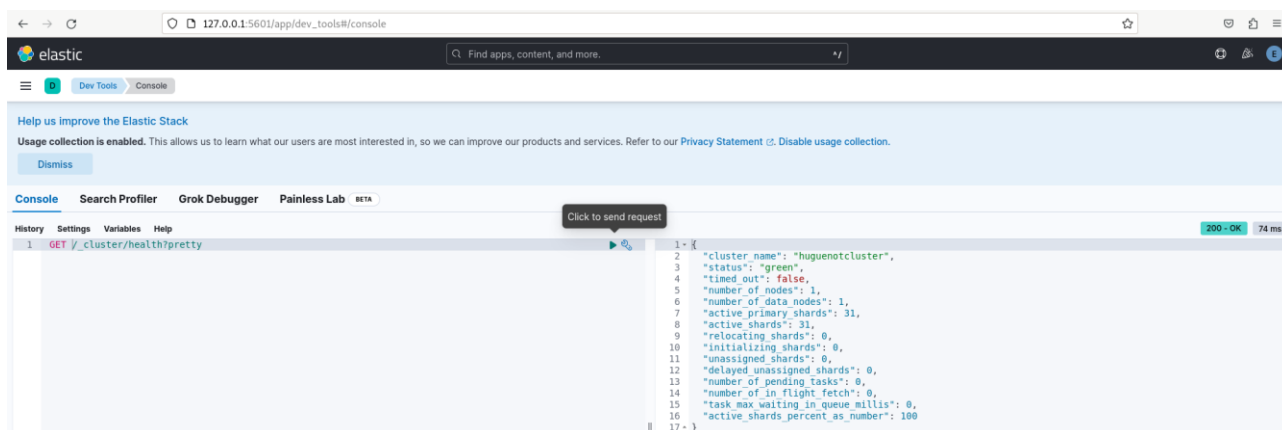


Рисунок 40 – Результат выполненного запроса

## 3 LOGTASH

### 3.1 Установка logstash

Выполним установку logstash при помощи команды: `apt install logstash`.  
Выполнение установки logstash отображено на рисунке 41

```
root@ZIVSYBD-LR4:/home/huguenot-lr4# apt install logstash
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  logstash
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 405 MB of archives.
After this operation, 669 MB of additional disk space will be used.
Get:1 http://elasticrepo.serveradmin.ru bullseye/main amd64 logstash amd64 1:8.13.3-1 [405 MB]
Fetched 405 MB in 43s (9,441 kB/s)
Selecting previously unselected package logstash.
(Reading database ... 257524 files and directories currently installed.)
Preparing to unpack .../logstash_1%3a8.13.3-1_amd64.deb ...
Unpacking logstash (1:8.13.3-1) ...
Setting up logstash (1:8.13.3-1) ...
root@ZIVSYBD-LR4:/home/huguenot-lr4#
```

Рисунок 41 – Выполнение установки logstash

Добавим logstash в автозагрузку при помощи команды `systemctl enable logstash.service`. Добавление logstash в автозагрузку отображено на рисунке 42

```
root@ZIVSYBD-LR4:/home/huguenot-lr4# systemctl enable logstash.service
Created symlink /etc/systemd/system/multi-user.target.wants/logstash.service → /lib/systemd/system/logstash.service.
root@ZIVSYBD-LR4:/home/huguenot-lr4#
```

Рисунок 42 – Добавление logstash в автозагрузку

### 3.2 Настройка logstash

Выполним настройку logstash перейдя в папку при помощи команды: `cd /etc/logstash/conf.d` и создадим файл `touch input.conf`. Переход в папку `conf.d` и создание файла `input.conf` отображено на рисунке 43

```
root@ZIVSYBD-LR4:/home/huguenot-lr4# cd /etc/logstash/conf.d
root@ZIVSYBD-LR4:/etc/logstash/conf.d# touch input.conf
```

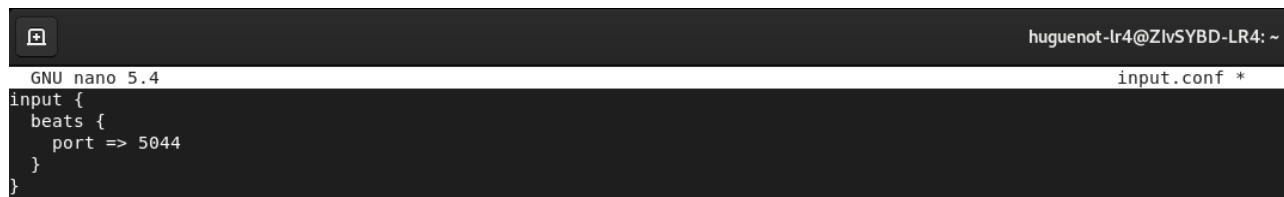
Рисунок 43 – Переход в папку `conf.d` и создание файла `input.conf`

Откроем созданный файл `conf.d` при помощи команды `nano input.conf`.  
Открытие файла `conf.d` отображено на рисунке 44

```
root@ZivSYBD-LR4:/etc/logstash/conf.d# nano input.conf
```

Рисунок 44 – Открытие файла input.conf

Конфигурация файла input.conf отображена на рисунке 45



```
huguenot-lr4@ZivSYBD-LR4: ~
GNU nano 5.4 input.conf *
input {
  beats {
    port => 5044
  }
}
```

Рисунок 45 – Открытие файла input.conf

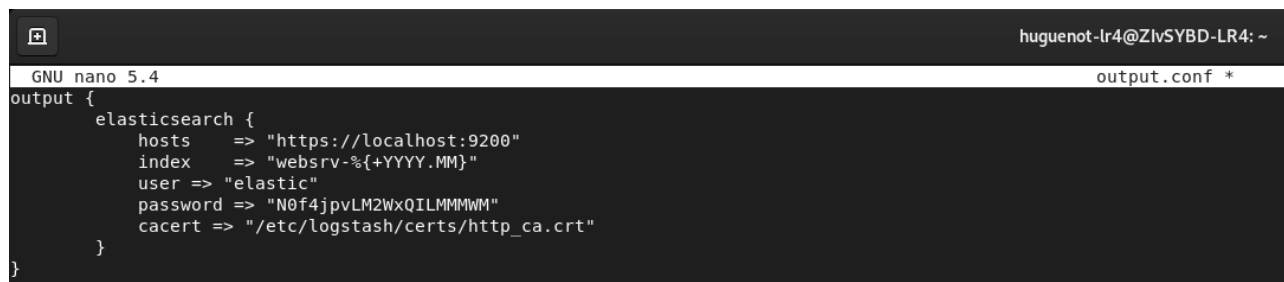
Создадим файл output.conf при помощи команды: touch output.conf.

Создание файла output.conf отображено на рисунке 46

```
root@ZivSYBD-LR4:/etc/logstash/conf.d# touch output.conf
```

Рисунок 46 - Создание файла output.conf

Конфигурация файла output.conf отображена на рисунке 47



```
huguenot-lr4@ZivSYBD-LR4: ~
GNU nano 5.4 output.conf *
output {
  elasticsearch {
    hosts => "https://localhost:9200"
    index => "websrv-%{+YYYY.MM}"
    user => "elastic"
    password => "N0f4jpvLM2WxQILMMWMM"
    cacert => "/etc/logstash/certs/http_ca.crt"
  }
}
```

Рисунок 47 – Конфигурация файла output.conf

Выполним копирование сертификатов и назначим права при помощи команд: cp -R /etc/elasticsearch/certs /etc/logstash и chown -R root:logstash /etc/logstash/certs. Копирование сертификатов и назначение прав отображено на рисунке 48

```
root@ZivSYBD-LR4:/etc/logstash/conf.d# cp -R /etc/elasticsearch/certs /etc/logstash
root@ZivSYBD-LR4:/etc/logstash/conf.d# chown -R root:logstash /etc/logstash/certs
root@ZivSYBD-LR4:/etc/logstash/conf.d#
```

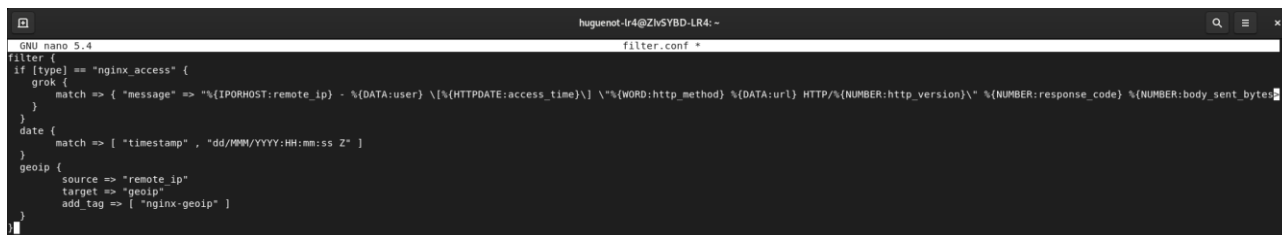
Рисунок 48 – Копирование сертификатов и назначение прав

При помощи команды: `touch` создадим файл `filter.conf`. Создание файла `filter.conf` отображено на рисунке 49

```
root@ZivSYBD-LR4:/etc/logstash/conf.d# touch filter.conf
root@ZivSYBD-LR4:/etc/logstash/conf.d# nano filter.conf
```

Рисунок 49 – Создание файла `filter.conf`

Конфигурация файла `filter.conf` отображена на рисунке 50

A screenshot of a terminal window with a dark background. The title bar shows 'huguenot-lr4@ZivSYBD-LR4: -'. The terminal content shows the nano 5.4 editor editing the file 'filter.conf'. The configuration is as follows:

```
filter {
  if [type] == "nginx_access" {
    grok {
      match => { "message" => "%{[IPORHOST:remote_ip]} - %{[DATA:user]} \[%{[HTTPDATE:access_time]}\] \"%{[WORD:http_method]} %{[DATA:url]} HTTP/%{[NUMBER:http_version]}\" %{[NUMBER:response_code]} %{[NUMBER:body_sent_bytes]}"}
    }
  }
  date {
    match => [ "timestamp" , "dd/MMM/YYYY:HH:mm:ss Z" ]
  }
  geoip {
    source => "remote_ip"
    target => "geoip"
    add_tag => [ "nginx-geoip" ]
  }
}
```

Рисунок 50 – Конфигурация файла `filter.conf`

Настройка `logstash` завершена. Перезапустим `logstash` при помощи команды: `systemctl start logstash.service`. Перезапуск `logstash` отображен на рисунке 51

```
root@ZivSYBD-LR4:/etc/logstash/conf.d# systemctl start logstash.service
root@ZivSYBD-LR4:/etc/logstash/conf.d#
```

Рисунок 51 – Перезапуск `logstash`

При помощи команды: `cat /var/log/logstash/logstash-plain.log` проверим лог `logstash`. Лог `logstash` отображен на рисунке 52

```
Activities Terminal Jun 5 15:24 huguenot-lr4@ZNV5BD-LR4: -
ber-length=10000, -Djruby.rexepx.interruptible=true, -Djdk.io.File.enableADS=true, --add-exports=jdk.compiler/com.sun.tools.javac.api=ALL-UNNAMED, --add-exports=jdk.compiler/com.sun.tools.javac.file=ALL-UNNAMED,
--add-exports=jdk.compiler/com.sun.tools.javac.parser=ALL-UNNAMED, --add-exports=jdk.compiler/com.sun.tools.javac.tree=ALL-UNNAMED, --add-exports=jdk.compiler/com.sun.tools.javac.util=ALL-UNNAMED, --add-opens=java.base/java.security=ALL-UNNAMED, --add-opens=java.base/java.io=ALL-UNNAMED, --add-opens=java.base/java.nio.channels=ALL-UNNAMED, --add-opens=java.base/sun.nio.ch=ALL-UNNAMED, --add-opens=java.management/sun.m
management=ALL-UNNAMED, -Dio.netty.allocation.maxOrder=11]
[2024-06-05T15:23:22,998][INFO ][logstash.runner] Jackson default value override 'logstash.jackson.stream-read-constraints.max-string-length' configured to '200000000'
[2024-06-05T15:23:22,998][INFO ][logstash.runner] Jackson default value override 'logstash.jackson.stream-read-constraints.max-number-length' configured to '10000'
[2024-06-05T15:23:23,015][INFO ][logstash.settings] Creating directory (:settings='path.queue', :path='/var/lib/logstash/queue')
[2024-06-05T15:23:23,017][INFO ][logstash.settings] Creating directory (:settings='path.dead.letter.queue', :path='/var/lib/logstash/dead.letter.queue')
[2024-06-05T15:23:23,237][INFO ][logstash.agent] No persistent UUID file found. Generating new UUID (:uuid='19elbcd9-dec2-4a29-bc04-6ea0755d5dfe', :path='/var/lib/logstash/uuid')
[2024-06-05T15:23:23,750][INFO ][logstash.agent] Successfully started Logstash APT endpoint (:port=9600, :ssl.enabled=false)
[2024-06-05T15:23:24,360][INFO ][org.reflections.Reflections] Reflections took 106 ms to scan 1 urls, producing 132 keys and 468 values
[2024-06-05T15:23:24,740][WARN ][logstash.outputs.elasticsearch] You are using a deprecated config setting 'cacert' set in elasticsearch. Deprecated settings will continue to work, but are scheduled for removal from logstash in the future. Set 'ssl.certificate.authorities' instead. If you have any questions about this, please visit the #logstash channel on freenode irc. {:names=>'cacert', :plugin=>'Logstash::Outputs::ElasticSearch', :index=>'webstv-%{YYYY.MM}', :password=>'password', :id=>'5c79ac93c82f5b6e67633c76660e25f88422149a1a0958669123efc401af0b48', :user=>'elastic', :hosts=>['https://localhost:9200'], :cacert=>'/etc/logstash/certs/http.ca.crt', :enable_metric=>true, :codec=>'Logstash::Codecs::Plain', :id=>'plain.9e5f57d2-0445-43ed-b30b-502ce832d620', :enable_metric=>true, :charset=>'UTF-8', :workers=>1, :ssl.certificate_verification=>true, :ssl_verification_modes=>'full', :sniffing.delay=>5, :timeout=>60, :pool.max=>1000, :pool.max.per.route=>100, :resurrect.delay=>5, :validate_after_inactivity=>10000, :http.compression=>true, :compression.level=>1, :retry.initial.intervals=>2, :retry.max.interval=>64, :dlq.on.failed.index.name_interpolations=>true, :data_stream.type=>'logs', :data_stream.dataset=>'generic', :data_stream.namespace=>'default', :data_stream.sync.fields=>true, :data_stream.auto.routing=>true, :manage.template=>true, :template.override=>false, :template.api=>'auto', :doc.as.upsert=>false, :script.type=>'inline', :script.lang=>'painless', :script.var.name=>'even', :scripted.upsert=>false, :retry.on.conflict=>1, :ilm.enabled=>'auto', :ilm.pattern=>'(now/d)-000001', :ilm.policy=>'logstash-policy'}
[2024-06-05T15:23:24,767][INFO ][logstash.javapipeline] Pipeline 'main' is configured with 'pipeline.ecs_compatibility: v8' setting. All plugins in this pipeline will default to 'ecs_compatibility => v8' unless explicitly configured otherwise.
[2024-06-05T15:23:24,781][INFO ][logstash.outputs.elasticsearch][main] New Elasticsearch output {:class=>'Logstash::Outputs::ElasticSearch', :hosts=>['https://localhost:9200']}
[2024-06-05T15:23:24,864][INFO ][logstash.outputs.elasticsearch][main] Elasticsearch pool URLs updated {:changes=>{:removed=>[], :added=>['https://elastic:xxxxxx@localhost:9200/']}}
[2024-06-05T15:23:25,091][WARN ][logstash.outputs.elasticsearch][main] Restored connection to ES instance (:url='https://elastic:xxxxxx@localhost:9200/')
[2024-06-05T15:23:25,092][INFO ][logstash.outputs.elasticsearch][main] Elasticsearch version determined (8.13.3) (:es.version=>8)
[2024-06-05T15:23:25,093][WARN ][logstash.outputs.elasticsearch][main] Detected a 6.x and above cluster: the 'type' event field won't be used to determine the document type (:es.version=>8)
[2024-06-05T15:23:25,102][INFO ][logstash.outputs.elasticsearch][main] Not eligible for data streams because config contains one or more settings that are not compatible with data streams: {:index=>'webstv-%{YYYY.MM}'}
[2024-06-05T15:23:25,103][INFO ][logstash.outputs.elasticsearch][main] Data streams auto configuration ('data_stream' => 'auto' or unset) resolved to 'false'
[2024-06-05T15:23:25,106][WARN ][logstash.filters.grok] [main] ECS v8 support is a preview of the unreleased ECS v8, and uses the v1 patterns. When Version 8 of the Elastic Common Schema becomes available, this plugin will need to be updated
[2024-06-05T15:23:25,110][INFO ][logstash.outputs.elasticsearch][main] Using a default mapping template (:es.version=>8, :ecs_compatibility=>v8)
[2024-06-05T15:23:25,159][INFO ][logstash.outputs.elasticsearch][main] Installing Elasticsearch template (:name=>'ecs-logstash')
[2024-06-05T15:23:25,163][INFO ][logstash.filters.geopip] [main] ECS expect 'target' value geopip in ['client', 'destination', 'host', 'observer', 'server', 'source']
[2024-06-05T15:23:31,902][INFO ][logstash.geopipdatamanager.manager] managed geopip database has been updated on disk (:database.type=>'ASN', :database.path=>'/var/lib/logstash/geopip_database_management/1717590205/GeoLite2-ASN.mmdb')
[2024-06-05T15:23:32,041][INFO ][logstash.geopipdatamanager.manager] managed geopip database has been updated on disk (:database.type=>'City', :database.path=>'/var/lib/logstash/geopip_database_management/1717590205/GeoLite2-City.mmdb')
[2024-06-05T15:23:32,058][INFO ][logstash.filters.geopipdatamanager.manager] By not manually configuring a database path with 'database =>', you accepted and agreed MaxMind EULA. For more details please visit https://www.maxmind.com/en/geolite2/eula
[2024-06-05T15:23:32,058][INFO ][logstash.filters.geopip] [main] Using geopip database (:path=>'/var/lib/logstash/geopip_database_management/1717590205/GeoLite2-City.mmdb')
[2024-06-05T15:23:32,058][INFO ][logstash.javapipeline] [main] Starting pipeline (:pipeline.id=>'main', :pipeline.workers=>4, :pipeline.batch.size=>125, :pipeline.batch.delay=>50, :pipeline.max.inflight=>500, :pipeline.sources=>['/etc/logstash/conf.d/filter.conf', '/etc/logstash/conf.d/input.conf', '/etc/logstash/conf.d/output.conf'], :thread=>#<Thread:0x4478b8f9 /usr/share/logstash/logstash-core/lib/logstash/java_pipeline.rb:134 run>)
[2024-06-05T15:23:32,779][INFO ][logstash.javapipeline] [main] Pipeline Java execution initialization time ("seconds"=>0.69)
[2024-06-05T15:23:32,787][INFO ][logstash.inputs.beats] [main] Starting input listener (:address=>'0.0.0.0:5044')
[2024-06-05T15:23:32,796][INFO ][logstash.javapipeline] [main] Pipeline started (:pipeline.id=>'main')
[2024-06-05T15:23:32,822][INFO ][logstash.agent] Pipelines running (:count=>1, :running.pipelines=>[main], :non_running.pipelines=>[])
[2024-06-05T15:23:32,831][INFO ][org.logstash.beats.Server] [main][63f43849bb265a30e48d3463c4f8fc7d8c8487580a7c4de378a3609d9b5c705a] Starting server on port: 5044
root@ZNV5BD-LR4:/etc/logstash/conf.d#
```

Рисунок 52 – Лог logstash

Успешный запуск logstash отображен на рисунке 53

```
[2024-06-05T15:23:32,881][INFO ][org.logstash.beats.Server] [main][63f43849bb265a30e48d3463c4f8fc7d8c8487580a7c4de378a3609d9b5c705a] Starting server on port: 5044
```

Рисунок 53 – Успешный запуск logstash

### 3.3 Данный пункт зарезервирован под дополнительные настройки

## 4 NGINX

### 4.1 Установка и настройка nginx

Выполним установку nginx при помощи команды: `apt install nginx`.

Установка nginx отображена на рисунке 54

```
root@ZivSYBD-LR4:/home/huguenot-lr4# apt install nginx
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  geoip-database libgeoip1 libnginx-mod-http-geoip libnginx-mod-http-image-filter
  libnginx-mod-http-xslt-filter libnginx-mod-mail libnginx-mod-stream libnginx-mod-stream-geoip
  nginx-common nginx-core
Suggested packages:
  geoip-bin fcgiwrap nginx-doc
The following NEW packages will be installed:
  geoip-database libgeoip1 libnginx-mod-http-geoip libnginx-mod-http-image-filter
  libnginx-mod-http-xslt-filter libnginx-mod-mail libnginx-mod-stream libnginx-mod-stream-geoip nginx
  nginx-common nginx-core
0 upgraded, 11 newly installed, 0 to remove and 0 not upgraded.
Need to get 4,541 kB of archives.
After this operation, 13.4 MB of additional disk space will be used.
Do you want to continue? [Y/n]
```

Рисунок 54 – Установка nginx

Установленный nginx отображен на рисунке 55

```
Setting up libnginx-mod-http-xslt-filter (1.18.0-6.1+deb11u3) ...
Setting up libgeoip1:amd64 (1.6.12-7) ...
Setting up geoip-database (20191224-3) ...
Setting up libnginx-mod-mail (1.18.0-6.1+deb11u3) ...
Setting up libnginx-mod-http-image-filter (1.18.0-6.1+deb11u3) ...
Setting up libnginx-mod-stream (1.18.0-6.1+deb11u3) ...
Setting up libnginx-mod-stream-geoip (1.18.0-6.1+deb11u3) ...
Setting up libnginx-mod-http-geoip (1.18.0-6.1+deb11u3) ...
Setting up nginx-core (1.18.0-6.1+deb11u3) ...
Upgrading binary: nginx.
Setting up nginx (1.18.0-6.1+deb11u3) ...
Processing triggers for man-db (2.9.4-2) ...
Processing triggers for libc-bin (2.31-13+deb11u10) ...
root@ZivSYBD-LR4:/home/huguenot-lr4#
```

Рисунок 55 – Установленный nginx

Добавим nginx в автозагрузку при помощи команды: `systemctl enable nginx`. Добавление nginx в автозагрузку отображено на рисунке 56

```
root@ZivSYBD-LR4:/home/huguenot-lr4# systemctl enable nginx
Synchronizing state of nginx.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable nginx
```

Рисунок 56 – Добавление nginx в автозагрузку



Запустим nginx при помощи команды: `systemctl start nginx`. Запуск nginx отображен на рисунке 57

```
root@ZiVSYBD-LR4:/home/huguenot-lr4# systemctl start nginx
```

Рисунок 57 – Запуск nginx

При помощи команды: `systemctl status nginx` проверим, запущен ли nginx. Проверка запуска nginx отображена на рисунке 58

```
root@ZiVSYBD-LR4:/home/huguenot-lr4# systemctl status nginx
● nginx.service - A high performance web server and a reverse proxy server
   Loaded: loaded (/lib/systemd/system/nginx.service; enabled; vendor preset: enabled)
   Active: active (running) since Wed 2024-06-05 15:41:15 MSK; 4min 22s ago
     Docs: man:nginx(8)
  Main PID: 23156 (nginx)
    Tasks: 5 (limit: 19095)
   Memory: 5.4M
      CPU: 54ms
   CGroup: /system.slice/nginx.service
           └─23156 nginx: master process /usr/sbin/nginx -g daemon on; master_process on;
              └─23159 nginx: worker process
                 └─23160 nginx: worker process
                    └─23161 nginx: worker process
                       └─23162 nginx: worker process

Jun 05 15:41:15 ZiVSYBD-LR4 systemd[1]: Starting A high performance web server and a reverse proxy server: nginx.
Jun 05 15:41:15 ZiVSYBD-LR4 systemd[1]: Started A high performance web server and a reverse proxy server.
```

Рисунок 58 - Проверка запуска nginx

Перейдем по адресу: `127.0.0.1:80`. Переход на адрес `127.0.0.1:80` отображен на рисунке 59



Рисунок 59 – Переход на адрес `127.0.0.1:80`

## 4.2 Отправка access-лог nginx в Elasticsearch с помощью Logstash

Для отправки access-лог nginx в Elasticsearch с помощью Logstash изменим файл конфигурации `input.conf`. Измененная конфигурация файла `input.conf` отображена на рисунке 60



Рисунок 60 – Измененная конфигурация файла input.conf

Остановим и запустим logstash.service при помощи команд `systemctl stop logstash.service` и `systemctl start logstash.service` тем самым выполнив перезапуск. Перезапуск logstash.service отображен на рисунке 61

```
root@ZivSYBD-LR4:~# systemctl stop logstash.service
root@ZivSYBD-LR4:~# systemctl start logstash.service
```

Рисунок 61 – Перезапуск logstash.service

При помощи команды: `cat /var/log/logstash/logstash-plain.log` проверим лог logstash. Лог logstash отображен на рисунке 62

```
[2024-06-05T16:01:36.712][WARN ][filewatch.tailmode.handlers.createinitial][main][047c40bdda1703ba5199060f511a2a120ebc2491ab4755b4e76e90d4ed2c6820] failed to open file {:path=>"/var/log/nginx/access.log", :exception=>Errno::EACCES, :message=>"Permission denied - /var/log/nginx/access.log"}
```

Рисунок 62 – Лог logstash

В логе logstash замечена ошибка на доступ к файлу из-за прав, по этой причине нету доступа к логам. Исправим ошибку выдав необходимые права при помощи команды: `sudo chmod o+r /var/log/nginx/access.log`. Выдача необходимых прав отображена на рисунке 63

```
root@ZivSYBD-LR4:~# sudo chmod o+r /var/log/nginx/access.log
```

Рисунок 63 – Выдача необходимых прав

Остановим и запустим logstash.service при помощи команд `systemctl stop logstash.service` и `systemctl start logstash.service` тем самым выполнив перезапуск. Перезапуск logstash.service отображен на рисунке 64

```
root@ZIVSYBD-LR4:~# systemctl stop logstash.service
root@ZIVSYBD-LR4:~# systemctl start logstash.service
```

Рисунок 64 – Перезапуск logstash.service

Перейдем в панель управления Elasticsearch. Переход в панель управления Elasticsearch отображен на рисунке 65

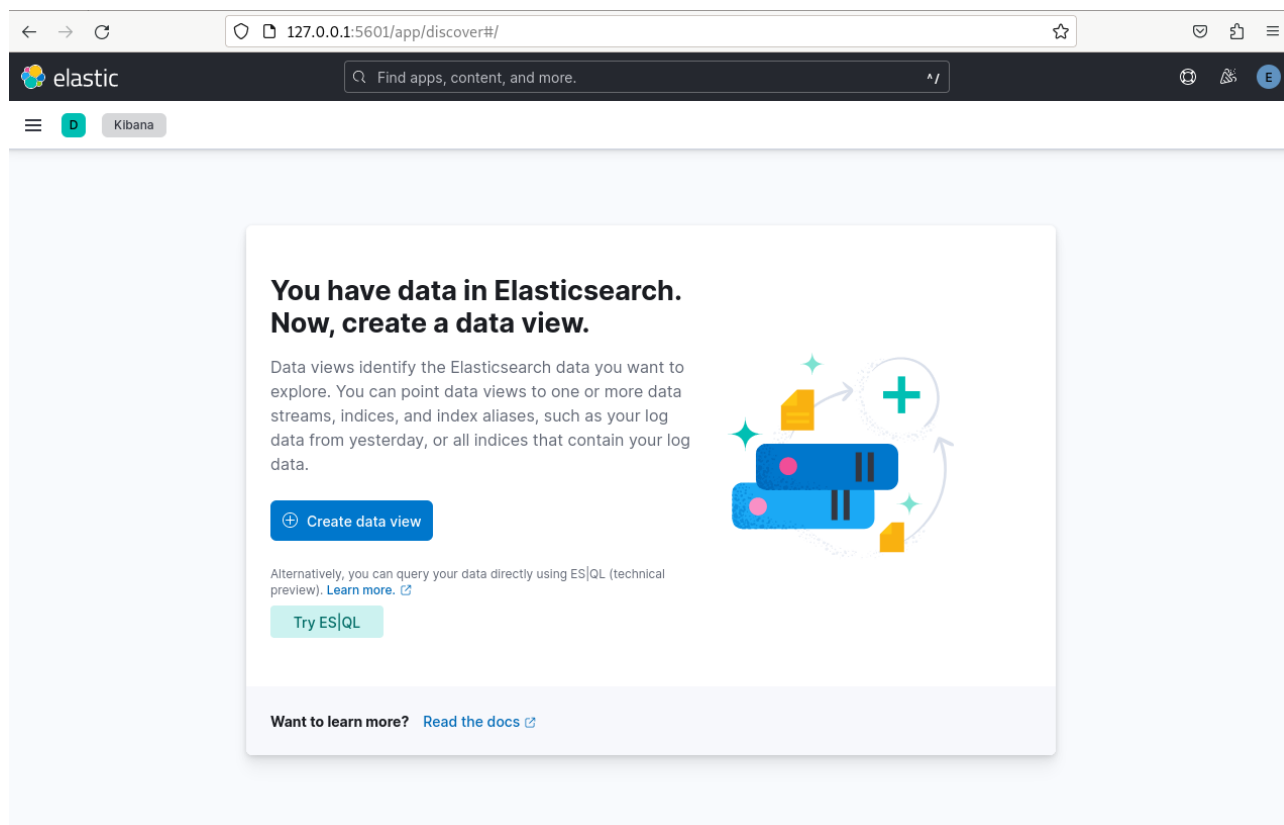


Рисунок 65 – Переход в панель управления Elasticsearch

Продолжим настройку. В поле name укажем nginx, а в поле index pattern укажем websrv-\*. Продолжение настроек отображено на рисунке 66

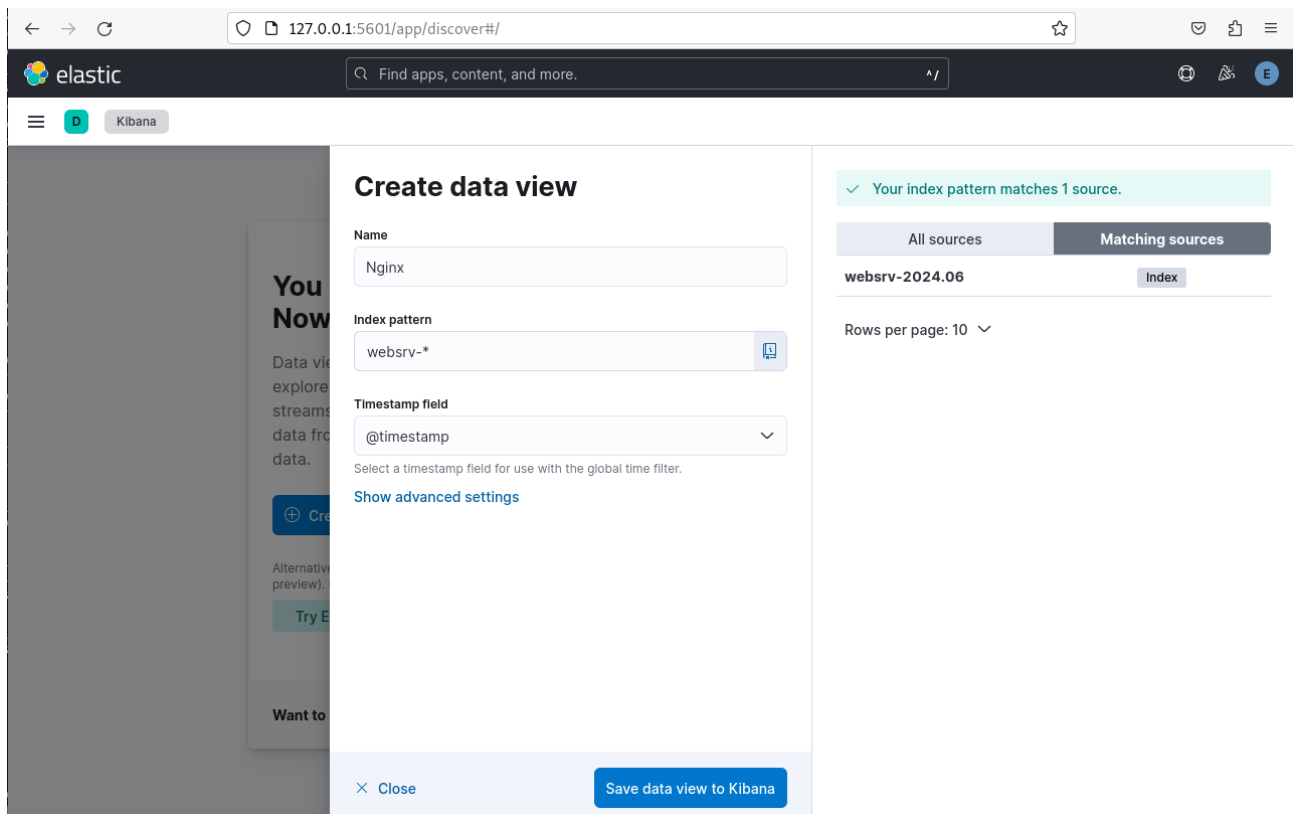


Рисунок 66 – Продолжение настроек

Перейдем в раздел Discover в который начали поступать логи от nginx. Поступающих логи отображены на рисунке 67

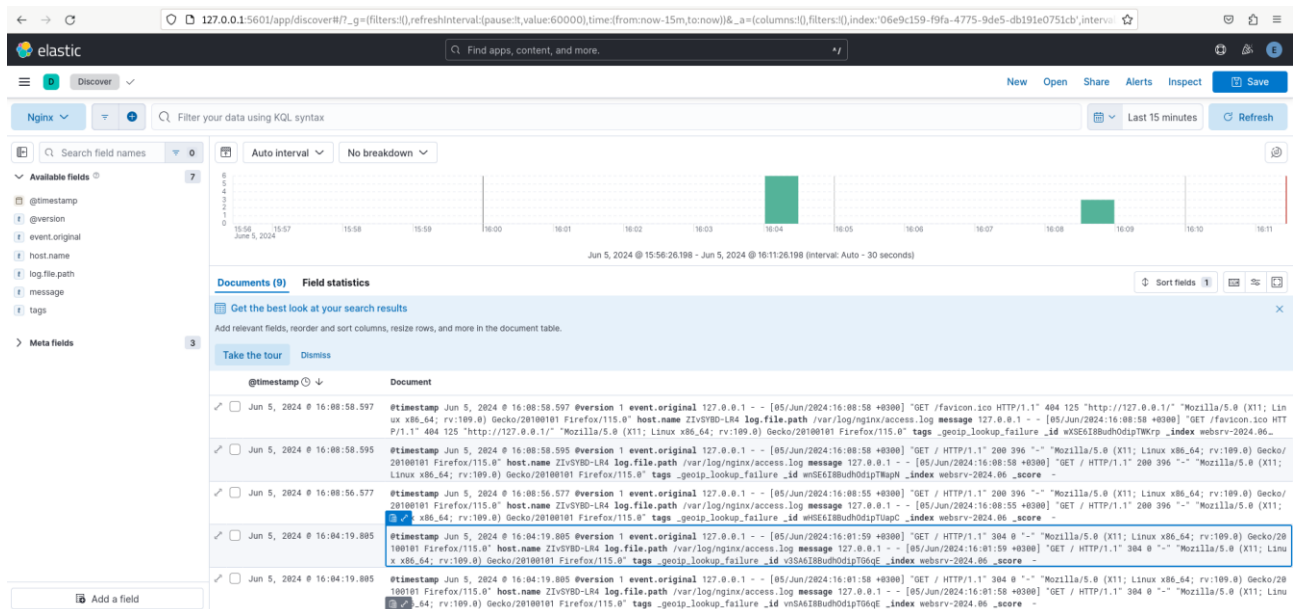


Рисунок 67 – Поступающие логи

# Логи nginx отображены на рисунке 68

Documents (9)Field statistics

Get the best look at your search results

Add relevant fields, reorder and sort columns, resize rows, and more in the document table.

Take the tourDismiss

@timestamp	Document
<input checked="" type="checkbox"/> Jun 5, 2024 @ 16:08:58.597	<pre>..._id : wXSE618BudhOdipTWKrp ,   "_score": 1,   "_source": null,   "fields": {     "event.original": [       "127.0.0.1 - - [05/Jun/2024:16:08:58 +0300] \"GET /favicon.ico HTTP/1.1\" 404 125 \"http://127.0.0.1/\" Mozilla/5.0 (X11; Lin ; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0\" tags_geoip_lookup_failure_id wXSE618BudhOdipTWKrp _index webserv-2024.06_ nt.original 127.0.0.1 - - [05/Jun/2024:16:08:58 +0300] \"GET / HTTP/1.1\" 200 396 \"-\" Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20 le.path /var/log/nginx/access.log message 127.0.0.1 - - [05/Jun/2024:16:08:58 +0300] \"GET / HTTP/1.1\" 200 396 \"-\" Mozilla/5.0 (X11; tags_geoip_lookup_failure_id wNSE618BudhOdipTWapN _index webserv-2024.06 _score - nt.original 127.0.0.1 - - [05/Jun/2024:16:08:55 +0300] \"GET / HTTP/1.1\" 200 396 \"-\" Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20 le.path /var/log/nginx/access.log message 127.0.0.1 - - [05/Jun/2024:16:08:55 +0300] \"GET / HTTP/1.1\" 200 396 \"-\" Mozilla/5.0 (X11; tags_geoip_lookup_failure_id v3SA618BudhOdipT06qE _index webserv-2024.06 _score - nt.original 127.0.0.1 - - [05/Jun/2024:16:01:59 +0300] \"GET / HTTP/1.1\" 304 0 \"-\" Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20 le.path /var/log/nginx/access.log message 127.0.0.1 - - [05/Jun/2024:16:01:59 +0300] \"GET / HTTP/1.1\" 304 0 \"-\" Mozilla/5.0 (X11; Linu ps_geoip_lookup_failure_id v3SA618BudhOdipT06qE _index webserv-2024.06 _score - nt.original 127.0.0.1 - - [05/Jun/2024:16:01:58 +0300] \"GET / HTTP/1.1\" 304 0 \"-\" Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20 le.path /var/log/nginx/access.log message 127.0.0.1 - - [05/Jun/2024:16:01:58 +0300] \"GET / HTTP/1.1\" 304 0 \"-\" Mozilla/5.0 (X11; Linu tags_geoip_lookup_failure_id vnSA618BudhOdipT06qE _index webserv-2024.06 _score -</pre>
<input type="checkbox"/> Jun 5, 2024 @ 16:08:58.595	
<input type="checkbox"/> Jun 5, 2024 @ 16:08:56.577	
<input checked="" type="checkbox"/> Jun 5, 2024 @ 16:04:19.805	
<input type="checkbox"/> Jun 5, 2024 @ 16:04:19.805	

Рисунок 68 – Логи nginx

## 5 FILEBEAT ДЛЯ ОТПРАВКИ ЛОГОВ В LOGSTASH

### 5.1 Установка filebeat

Выполним установку filebeat при помощи команды: `apt install filebeat`.

Установка filebeat отображена на рисунке 69

```
root@ZIVSYBD-LR4:~# apt install filebeat
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  filebeat
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 51.0 MB of archives.
After this operation, 188 MB of additional disk space will be used.
Get:1 http://elasticrepo.serveradmin.ru bullseye/main amd64 filebeat amd64 8.13.3 [51.0 MB]
Fetched 51.0 MB in 6s (8,207 kB/s)
Selecting previously unselected package filebeat.
(Reading database ... 272293 files and directories currently installed.)
Preparing to unpack .../filebeat_8.13.3_amd64.deb ...
Unpacking filebeat (8.13.3) ...
Setting up filebeat (8.13.3) ...
root@ZIVSYBD-LR4:~#
```

Рисунок 69 – filebeat

### 5.2 Настройка filebeat

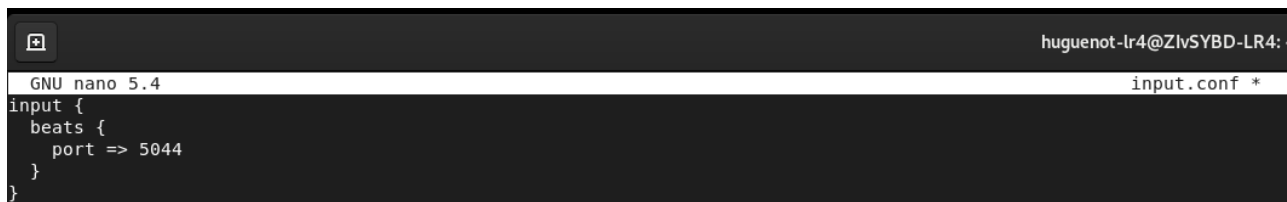
Для настройки filebeat вернемся к редактированию файла конфигурации logstash. Удалим активную конфигурацию и раскомментируем предыдущую. Изменение файла конфигурации logstash отображено на рисунке 70

```
huguenot-lr4@ZIVSYBD-LR4: ~
GNU nano 5.4 input.conf
#input {
#  beats {
#    port => 5044
#  }
#}

input {
  file {
    path => "/var/log/nginx/access.log"
    start_position => "beginning"
  }
}
```

Рисунок 70 – Изменение файла конфигурации

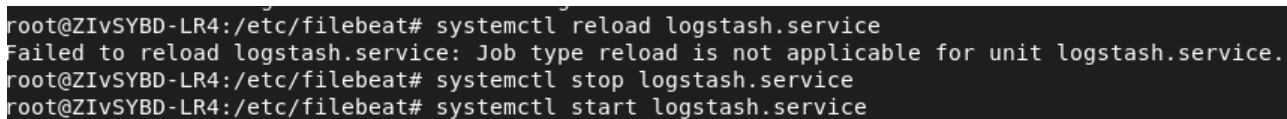
Измененная конфигурация logstash файла `input.conf` отображена на рисунке 71



```
GNU nano 5.4 input.conf *
input {
  beats {
    port => 5044
  }
}
```

Рисунок 71 – Измененная конфигурация logstash файла input.conf

Для вступления изменений в силу выполним перезагрузку logstash при помощи команды: `systemctl reload logstash.service`. Выполнение перезагрузки logstash отображено на рисунке 72

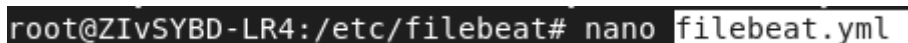


```
root@ZIVSYBD-LR4:/etc/filebeat# systemctl reload logstash.service
Failed to reload logstash.service: Job type reload is not applicable for unit logstash.service.
root@ZIVSYBD-LR4:/etc/filebeat# systemctl stop logstash.service
root@ZIVSYBD-LR4:/etc/filebeat# systemctl start logstash.service
```

Рисунок 72 – Выполнение перезагрузки logstash

### 5.3 Настройка поставки логов через filebeat

Выполним настройку конфигурационного файла `filebeat.yml` находящегося в директории `/etc/filebeat` при помощи команды `nano`. Открытие файла конфигурации отображено на рисунке 73



```
root@ZIVSYBD-LR4:/etc/filebeat# nano filebeat.yml
```

Рисунок 73 – Открытие файла конфигурации

В разделе `filebeat inputs` файла конфигурации `filebeat.yml` установим значение `enable` на `true`. Укажем путь до файла с логами `nginx`. Редактирование раздела `filebeat inputs` файла конфигурации `filebeat.yml` отображено на рисунке 74

```
# ===== Filebeat inputs =====

filebeat.inputs:

# Each - is an input. Most options can be set at the input level, so
# you can use different inputs for various configurations.
# Below are the input-specific configurations.

# filestream is an input for collecting log messages from files.
- type: filestream

  # Unique ID among all inputs, an ID is required.
  id: my-filestream-id

  # Change to true to enable this input configuration.
  enabled: true

  # Paths that should be crawled and fetched. Glob based paths.
  paths:
    - /var/log/nginx/*-access.log
    #- c:\programdata\elasticsearch\logs\*
```

Рисунок 74 – Редактирование раздела filebeat inputs файла конфигурации  
filebeat.yml

В разделе filebeat modules файла конфигурации filebeat.yml оставляем все значения без изменений Редактирование раздела filebeat modules файла конфигурации filebeat.yml отображено на рисунке 75

```
# ===== Filebeat modules =====

filebeat.config.modules:
  # Glob pattern for configuration loading
  path: ${path.config}/modules.d/*.yaml

  # Set to true to enable config reloading
  reload.enabled: false

  # Period on which files under path should be checked for changes
  #reload.period: 10s

# ===== Elasticsearch template setting =====

setup.template.settings:
  index.number_of_shards: 1
  #index.codec: best_compression
  #_source.enabled: false
```

Рисунок 75 – Редактирование раздела filebeat modules файла конфигурации  
filebeat.yml



В разделе outputs файла конфигурации filebeat.yml необходимо обязательно закомментировать строки относящиеся к elasticsearch иначе при запуске возникнет ошибка не позволяющая передавать логи. Строки logstash необходимо раскомментировать и указать ip адрес или localhost в нашем случае. Редактирование раздела outputs файла конфигурации filebeat.yml отображено на рисунке 76

```
# ===== Outputs =====  
  
# Configure what output to use when sending the data collected by the beat.  
  
# ----- Elasticsearch Output -----  
#output.elasticsearch:  
# Array of hosts to connect to.  
#hosts: ["localhost:9200"]  
  
# Performance preset - one of "balanced", "throughput", "scale",  
# "latency", or "custom".  
#preset: balanced  
  
# Protocol - either `http` (default) or `https`.  
#protocol: "https"  
  
# Authentication credentials - either API key or username/password.  
#api_key: "id:api_key"  
#username: "elastic"  
#password: "changeme"  
  
# ----- Logstash Output -----  
output.logstash:  
# The Logstash hosts  
hosts: ["localhost:5044"]  
  
# Optional SSL. By default is off.  
# List of root certificates for HTTPS server verifications  
#ssl.certificate_authorities: ["/etc/pki/root/ca.pem"]  
  
# Certificate for SSL client authentication  
#ssl.certificate: "/etc/pki/client/cert.pem"  
  
# Client Certificate Key  
#ssl.key: "/etc/pki/client/cert.key"
```

Рисунок 76 – Редактирование раздела outputs файла конфигурации filebeat.yml

В разделе processor файла конфигурации filebeat.yml конфигурацию оставляем без изменений. Редактирование раздела outputs файла конфигурации filebeat.yml отображено на рисунке 77

```
# ===== Processors =====
processors:
  - add_host_metadata:
      when.not.contains.tags: forwarded
  - add_cloud_metadata: ~
  - add_docker_metadata: ~
  - add_kubernetes_metadata: ~

# ===== Logging =====
```

Рисунок 77 – Редактирование раздела outputs файла конфигурации filebeat.yml

Добавим filebeat в автозагрузку при помощи команды: `systemctl enable --now filebeat`. Добавление filebeat в автозагрузку отображено на рисунке 78

```
root@ZIVSYBD-LR4:/etc/filebeat# systemctl enable --now filebeat
Synchronizing state of filebeat.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable filebeat
Created symlink /etc/systemd/system/multi-user.target.wants/filebeat.service → /lib/systemd/system/filebeat.service.
root@ZIVSYBD-LR4:/etc/filebeat#
```

Рисунок 78 – Добавление filebeat в автозагрузку

Проверим статус filebeat при помощи команды `systemctl status filebeat`. Проверка статуса filebeat отображена на рисунке 79

```
root@ZIVSYBD-LR4:/etc/filebeat# nano filebeat.yml
root@ZIVSYBD-LR4:/etc/filebeat# systemctl stop filebeat
root@ZIVSYBD-LR4:/etc/filebeat# systemctl start filebeat
root@ZIVSYBD-LR4:/etc/filebeat# systemctl status filebeat
● filebeat.service - Filebeat sends log files to Logstash or directly to Elasticsearch.
   Loaded: loaded (/lib/systemd/system/filebeat.service; enabled; vendor preset: enabled)
   Active: active (running) since Thu 2024-06-06 18:06:00 MSK; 2s ago
     Docs: https://www.elastic.co/beats/filebeat
   Main PID: 41503 (filebeat)
      Tasks: 9 (limit: 19695)
     Memory: 41.3M
        CPU: 324ms
   CGroup: /system.slice/filebeat.service
           └─41503 /usr/share/filebeat/bin/filebeat --environment systemd -c /etc/filebeat/filebeat.yml --path.home /usr/share/filebeat --path.config /etc/filebeat --path.data /var/lib/filebeat --path.logs /
```

Рисунок 79 – Проверка статуса filebeat

Filebeat запущен и работает. Все данные об log access nginx передаются в elasticsearch. Вернемся в панель elasticsearch, обновим страницу. Данные log access nginx поступают исправно. Поступающие данные log access nginx отображены на рисунке 80

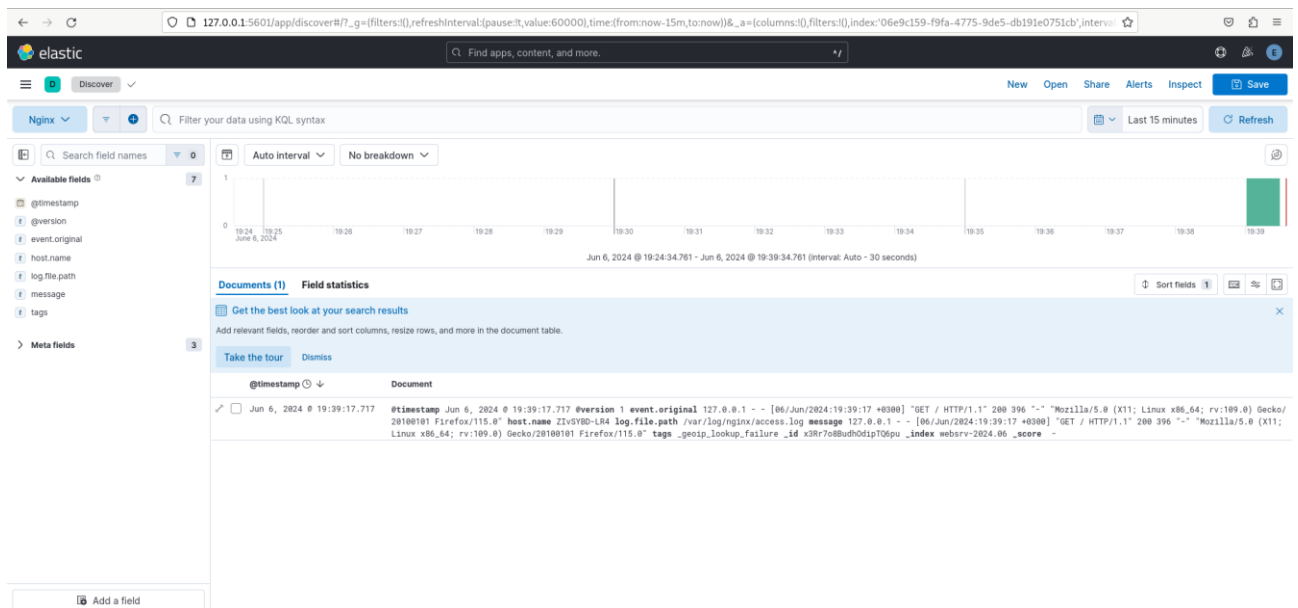


Рисунок 80 – Поступающие данные log access nginx

Один из логов nginx access приведен на рисунке 81

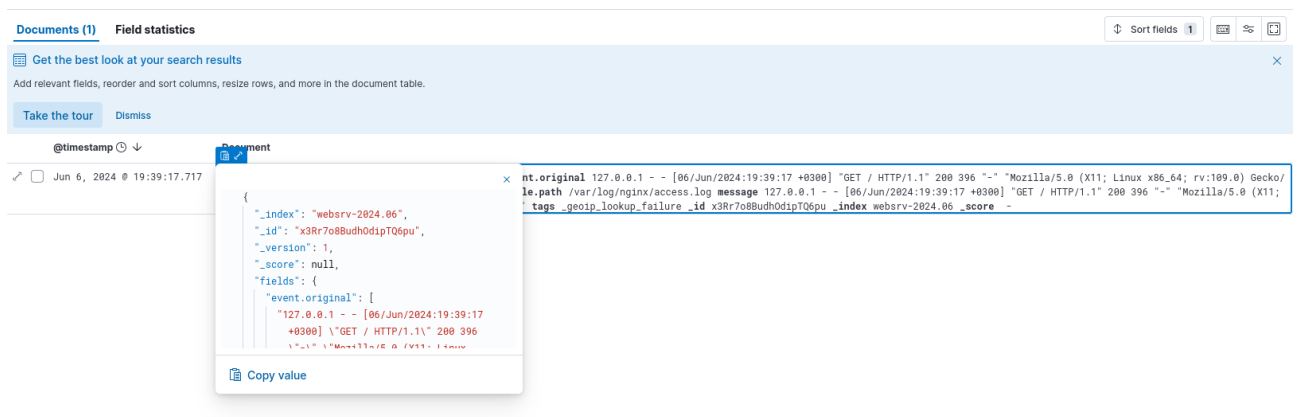


Рисунок 81 – Лог nginx access

## 6 НАСТРОЙКА ПОСТАВКИ ЛОГА В ELASTICSEARCH ЧЕРЕЗ LOGSTASH И FILEBEAT

6.1 Раздел был зарезервирован для настройки поставки логов с Windows при помощи Winlogbeat

Во время настройки возникли неполадки не позволяющие продолжить сбор и поставку логов при помощи Winlogbeat в Elasticsearch. Описательная часть отсутствует

### 6.2 Парсинг лога и разложение на поля

Дополнительный раздел к предыдущим пунктам, описывающий процесс парсинга лога и разложение его на поля

```
{
  "@timestamp": [
    "2024-06-06T16:39:17.717Z"
  ],
  "@version": [
    "1"
  ],
  "@version.keyword": [
    "1"
  ],
  "event.original": [
    "127.0.0.1 - - [06/Jun/2024:19:39:17 +0300] \"GET / HTTP/1.1\" 200 396 \"-\" \"Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0\""
  ],
  "event.original.keyword": [
    "127.0.0.1 - - [06/Jun/2024:19:39:17 +0300] \"GET / HTTP/1.1\" 200 396 \"-\" \"Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0\""
  ],
  "host.name": [
    "ZIVSYBD-LR4"
  ],
  "host.name.keyword": [
    "ZIVSYBD-LR4"
  ],
  "log.file.path": [
    "/var/log/nginx/access.log"
  ],
  "log.file.path.keyword": [
    "/var/log/nginx/access.log"
  ],
  "message": [
    "127.0.0.1 - - [06/Jun/2024:19:39:17 +0300] \"GET / HTTP/1.1\" 200 396 \"-\" \"Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0\""
  ],
  "message.keyword": [
```

```
"127.0.0.1 - - [06/Jun/2024:19:39:17 +0300] \"GET / HTTP/1.1\" 200 396 \"-\"  
\"Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0\"  
],  
  \"tags\": [  
    \"_geoip_lookup_failure\"  
  ],  
  \"tags.keyword\": [  
    \"_geoip_lookup_failure\"  
  ],  
  \"_id\": \"x3Rr7o8BudhOdipTQ6pu\",  
  \"_index\": \"websrv-2024.06\",  
  \"_score\": null  
}
```

## 6.3 Изменение файлов конфигурации

### 6.3.1 Изменение файла конфигурации

### 6.3.2 Изменение файла конфигурации

### 6.3.3 Изменение файла конфигурации

### 6.3.4 Изменение файла конфигурации

## 6.4 Проверка поступающих логов в ElasticSearch

## КОНТРОЛЬНЫЕ ВОПРОСЫ

## ВЫВОД

В ходе выполнения лабораторной работы по теме: «ELK» получили практический навык при работе с ELK